Kyle McLean (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney*
Email: mbarney@sirillp.com
Tyler Bean*
Email: tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Attorneys for Plaintiff and the Nationwide Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN ROSSI, MICHAEL THOMAS, and MARISSA PORTER, on behalf of themselves and all others similarly situated, Plaintiffs, v. **POSTMEDS, INC. d/b/a TRUEPILL,** Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs John Rossi, Michael Thomas, Marissa Porter ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Postmeds, Inc. d/b/a Truepill ("Postmeds" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Postmeds for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Postmeds patients' personally identifiable

information ("PII") and protected health information ("PHI"), including names, demographic information, prescription information, medication type, and prescribing physician (the "Private Information"), from criminal hackers.

2. Postmeds, based in Hayward, California, is a digital pharmacy company that fulfills prescriptions and dispenses medication to more than 3 million patients nationwide.

3. On or about October 31, 2023, Postmeds filed official notice of a hacking incident with the Attorney General of Texas.[1] Under state and federal law, organizations must report breaches involving protected health information within at least sixty (60) days.

4. On or about October 30, 2023, Postmeds also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice filed by Defendant, on August 31, 2023, unusual activity was detected on some of its computer systems. In response, Defendant launched an investigation. Postmeds' investigation revealed that an unauthorized party had access to certain files that contained sensitive patient information, and that such access took place between August 30, 2023, and September 1, 2023 (the "Data Breach").

6. Plaintiffs and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, names, demographic information, prescription information, medication type, and prescribing physician that Postmeds collected and maintained.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, using Class Members' names and Private Information to obtain medical services and/or prescription medication.

[1] *See* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Nov. 6, 2023).

9. There has been no assurance offered by Postmeds that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address Postmeds' inadequate safeguarding of Class Members' Private Information that it collected and maintained.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Postmeds, and thus Postmeds was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Postmeds and its employees failed to properly monitor and implement security practices with regard to its computer network and systems that housed the Private Information. Had Postmeds properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of Postmeds' negligent conduct as the Private Information that Postmeds collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence per se, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence, and declaratory judgment.

II. PARTIES

17. Plaintiff Rossi, is, and at all times mentioned herein was, an individual citizen of the State of Florida.

18. Plaintiff Thomas, is, and at all times mentioned herein was, an individual citizen of the State of Texas.

19. Plaintiff Porter, is, and at all times mentioned herein was, an individual citizen of the State of Florida.

20. Defendant Postmeds is a digital pharmacy company incorporated in Delaware with its principal place of business at 3121 Diablo Avenue, Hayward, California, 94545 in Alameda County.

III. JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Postmeds. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has jurisdiction over Postmeds because Postmeds operates in and/or is incorporated in this District.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Postmeds has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Postmeds' Business and Collection of Plaintiffs' and Class Members' Private Information

24. Postmeds is a digital healthcare company specializing in pharmacy delivery services. Founded in 2015, Postmeds operates a network of mail order and specialty pharmacies,

serving more than 3 million patients by shipping prescriptions to all fifty (50) states. Postmeds employs more than 300 people and generates approximately $101 million in annual revenue.

25. As a condition of receiving pharmaceutical services, Postmeds requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Postmeds, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

26. In its Notice of HIPAA Privacy Practices, Postmeds informs its patients that it is "required by law to maintain the privacy and security of your protected health information" and promises that it "will not use or share your information other than as described here unless you tell us we can in writing" and it will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[2] In addition, in its Privacy Policy, Postmeds promises its patients that it "respects your privacy and [is] committed to protecting it."[3]

27. Postmeds uses this information, *inter alia*, for research and business purposes.

28. Thus, due to the highly sensitive and personal nature of the information Postmeds acquires and stores with respect to its patients, Postmeds, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Postmeds assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

[2] *See* https://www.truepill.com/legal/nopp (last visited Nov. 6, 2023).
[3] *See* https://www.truepill.com/legal/privacy (last visited Nov. 6, 2023).

30. Plaintiffs and Class Members relied on Postmeds to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

31. According to Defendant's Notice, it learned of unauthorized access to its computer systems on August 31, 2023, with such unauthorized access having taken place between August 30, 2023, and September 1, 2023.

32. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, demographic information, prescription information, medication type, and prescribing physician.

33. On or about October 30, 2023, roughly two months after Postmeds learned that the Class's Private Information was first accessed by cybercriminals, Postmeds finally began to notify patients that its investigation determined that their Private Information was accessed.

34. Postmeds had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Plaintiffs and Class Members provided their Private Information to Postmeds with the reasonable expectation and mutual understanding that Postmeds would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

36. Postmeds' data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

37. Postmeds knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

38. Postmeds was on notice that companies in the healthcare industry are susceptible targets for data breaches.

39. Postmeds was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[4]

40. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[5]

41. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] In 2022, the largest growth in compromises occurred in the healthcare sector.[7]

42. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims

---

[4] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on Nov. 6, 2023).

[5] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Nov. 6, 2023).

[6] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on Nov. 6, 2023).

[7] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Nov. 6, 2023).

were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[8]

43. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[9]

44. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

45. As a healthcare provider, Postmeds knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Postmeds' patients as a result of a breach. Postmeds failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[8] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Nov. 6, 2023).

[9] *Id.*

[10] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Nov. 6, 2023).

D. Postmeds Failed to Comply with HIPAA

46. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

47. Postmeds' Data Breach resulted from a combination of insufficiencies that indicate Postmeds failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Postmeds' Data Breach that Postmeds either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

48. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

49. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

50. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

51. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

52. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

53. Based upon Defendant's Notice to Plaintiffs and Class Members, Postmeds reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

54. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

55. Postmeds reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

56. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

57. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

58. Postmeds reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

59. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

60. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

61. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

62. In addition, Postmeds' Data Breach could have been prevented if Postmeds had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

63. Postmeds' security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Postmeds creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

64. Because Postmeds has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Postmeds' approach to information security is adequate and appropriate going forward. Postmeds still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Postmeds Failed to Comply with FTC Guidelines

65. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

66. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating

someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. As evidenced by the Data Breach, Postmeds failed to properly implement basic data security practices. Postmeds' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

70. Postmeds was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Postmeds Failed to Comply with Industry Standards

71. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

72. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Postmeds include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees

can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

73. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

74. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

75. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Postmeds Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

76. In addition to its obligations under federal and state laws, Postmeds owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Postmeds owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

77. Postmeds breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Postmeds' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

78. Postmeds negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

79. Had Postmeds remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

80. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Postmeds.

H. Postmeds Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

81. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[11] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

82. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

83. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

84. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

[11] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Nov. 6, 2023).

Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

85. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

86. One such example of this is the development of "Fullz" packages.

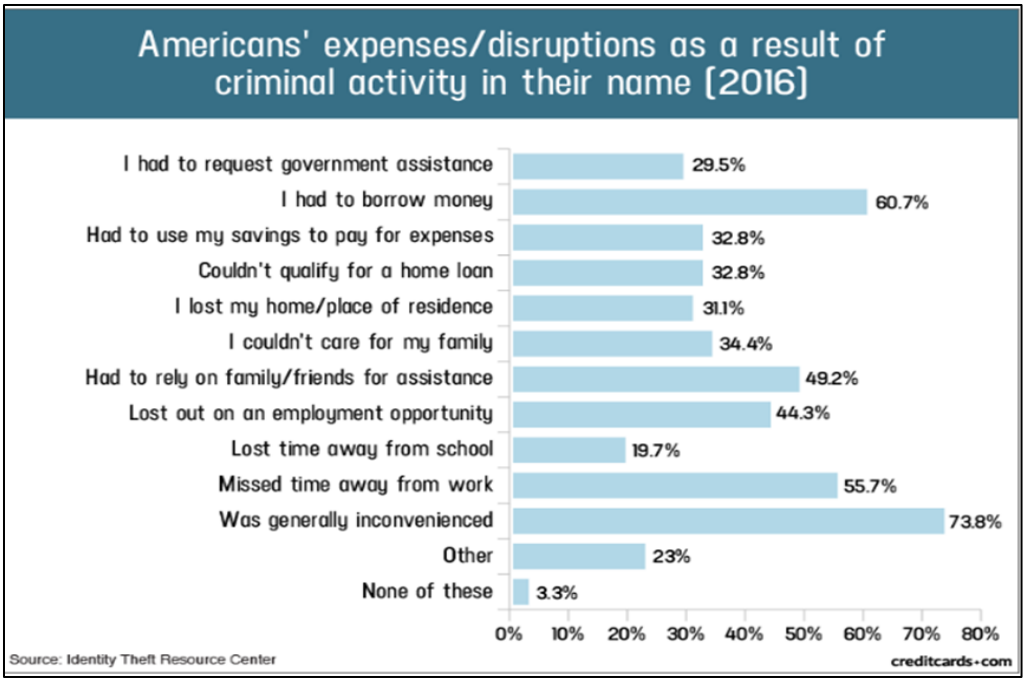
87. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

88. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

89. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[12] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

90. In fact, a study by the Identity Theft Resource Center[13] shows the multitude of harms caused by fraudulent use of PII:



91. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[14]

92. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

[12] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Nov. 6, 2023).

[13] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on Nov. 6, 2023).

[14] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Nov. 6, 2023).

93. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[15]

94. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

95. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

96. The ramifications of Postmeds' failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

97. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

98. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

[15] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Nov. 6, 2023).

[16] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Nov. 6, 2023).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[17]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

99. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

100. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiffs' and Class Members' Damages

Plaintiff Rossi's Experience

101. In order to receive pharmaceutical services, Defendant required Plaintiff Rossi provide it with substantial amounts of his PII and PHI.

102. On or about October 30, 2023, Plaintiff Rossi received a letter which told him that his PII and PHI had been accessed during the Data Breach. The notice letter informed him that the information stolen included his "name and prescription information."

103. The notice letter declined to offer Plaintiff any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Rossi will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

[17] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Nov. 6, 2023).

104. Plaintiff Rossi suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

105. Plaintiff Rossi would not have provided his PII and PHI to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

106. Plaintiff Rossi suffered actual injury in the form of having his PII and PHI compromised and/or stolen as a result of the Data Breach.

107. Plaintiff Rossi suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Rossi entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

108. Plaintiff Rossi suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

109. Plaintiff Rossi has a continuing interest in ensuring that his PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

110. As a result of the Data Breach, Plaintiff Rossi made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Rossi has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

111. As a result of the Data Breach, Plaintiff Rossi has suffered anxiety as a result of the release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of committing cyber and other crimes against him including,

but not limited to, medical fraud, and identity theft. Plaintiff Rossi is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

112. Plaintiff Rossi also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII and PHI, a form of property that Defendant obtained from Plaintiff Rossi; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

113. As a result of the Data Breach, Plaintiff Rossi anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Thomas' Experience

114. In order to receive pharmaceutical services, Defendant required Plaintiff Thomas provide it with substantial amounts of his PII and PHI.

115. On or about October 30, 2023, Plaintiff Thomas received a letter which told him that his PII and PHI had been accessed during the Data Breach. The notice letter informed him that the information stolen included his "name and prescription information."

116. The notice letter declined to offer Plaintiff Thomas any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Thomas will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

117. Plaintiff Thomas suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

118. Plaintiff Thomas would not have provided his PII and PHI to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices

to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

119. Plaintiff Thomas suffered actual injury in the form of having his PII and PHI compromised and/or stolen as a result of the Data Breach.

120. Plaintiff Thomas suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Thomas entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

121. Plaintiff Thomas suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

122. Plaintiff Thomas has a continuing interest in ensuring that his PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

123. As a result of the Data Breach, Plaintiff Thomas made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Thomas has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

124. As a result of the Data Breach, Plaintiff Thomas has suffered anxiety as a result of the release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of committing cyber and other crimes against him including, but not limited to, medical fraud, and identity theft. Plaintiff Thomas is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

125. Plaintiff Thomas also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the

value of his PII and PHI, a form of property that Defendant obtained from Plaintiff Thomas; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

126. As a result of the Data Breach, Plaintiff Thomas anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Porter's Experience

127. In order to receive pharmaceutical services, Defendant required Plaintiff Porter provide it with substantial amounts of her PII and PHI.

128. On or about October 30, 2023, Plaintiff Porter received a letter which told her that her PII and PHI had been accessed during the Data Breach. The notice letter informed her that the information stolen included her "name and prescription information."

129. The notice letter declined to offer Plaintiff Porter any complimentary credit monitoring services. Failing to offer credit monitoring is unacceptable given that Plaintiff Porter will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

130. Soon after the Data Breach, Plaintiff Porter suffered actual injury in the form of a substantial decrease in her credit score beginning on September 1, 2023, as well as the suspicious and unauthorized closure of two of her financial card accounts. In addition, she also suffered actual injury in the form of lost time spent dealing with the Data Breach and the increased risk of additional fraud, including medical fraud, resulting from the Data Breach, and monitoring her accounts for fraud.

131. Plaintiff Porter would not have provided her PII and PHI to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

132. Plaintiff Porter suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

133. Plaintiff Porter suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiff Porter entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

134. Plaintiff Porter suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

135. Plaintiff Porter has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

136. As a result of the Data Breach, Plaintiff Porter made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Porter has spent several hours dealing with the Data Breach, valuable times he otherwise would have spent on other activities.

137. As a result of the Data Breach, Plaintiff Porter has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, medical fraud, and identity theft. Plaintiff Porter is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

138. Plaintiff Porter also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendant obtained from Plaintiff Porter; (b)

violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

139. As a result of the Data Breach, Plaintiff Porter anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

140. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

141. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

142. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

143. As a direct and proximate result of Postmeds' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, and other forms of identity theft.

144. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including closely reviewing and monitoring insurance and other accounts and credit reports for unauthorized activity for years to come.

145. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

146. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information,

since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

147. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

148. Plaintiffs and Class Members also lost the benefit of the bargain they made with Postmeds. Plaintiffs and Class Members, directly or indirectly, overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to Postmeds was intended to be used by Postmeds to fund adequate security of Postmeds' system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

149. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[18] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[19]

150. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and

[18] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on November 7, 2023).

[19] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited November 7, 2023).

the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

151. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

152. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Postmeds, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

153. As a direct and proximate result of Postmeds' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

154. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

155. Specifically, Plaintiffs propose the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

156. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

157. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class before the Court determines whether certification is appropriate.

158. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

159. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of hundreds of thousands of Postmeds' patients whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Postmeds' records, Class Members' records, publication notice, self-identification, and other means.

160. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Postmeds engaged in the conduct alleged herein;

b. Whether Postmeds' conduct violated the FTCA and HIPAA;

c. When Postmeds learned of the Data Breach

d. Whether Postmeds' response to the Data Breach was adequate;

e. Whether Postmeds unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether Postmeds failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Postmeds' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Postmeds' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Postmeds owed a duty to Class Members to safeguard their Private Information;

j. Whether Postmeds breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Postmeds had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Postmeds breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Postmeds knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Postmeds' misconduct;

p. Whether Postmeds' conduct was negligent;

q. Whether Postmeds' conduct was *per se* negligent;

r. Whether Postmeds was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

161. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Postmeds. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

162. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

163. Predominance. Postmeds has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Postmeds' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

164. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Postmeds. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

165. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Postmeds has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

166. Finally, all members of the proposed Class are readily ascertainable. Postmeds has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Postmeds.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

167. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

168. Postmeds knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

169. Postmeds knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Postmeds was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

170. Postmeds owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Postmeds' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA.

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

171. Postmeds' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

172. Postmeds' duty also arose because Defendant was bound by industry standards to protect its patients' confidential Private Information.

173. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Postmeds owed them a duty of care to not subject them to an unreasonable risk of harm.

174. Postmeds, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Postmeds' possession.

175. Postmeds, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

176. Postmeds, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

177. Postmeds breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

178. Postmeds had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Postmeds with their Private Information was predicated on the understanding that Postmeds would take adequate security precautions. Moreover, only Postmeds had the ability to protect its systems (and the Private Information that it stored on them) from attack.

179. Postmeds' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

180. As a result of Postmeds' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

181. Postmeds' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

182. As a result of Postmeds' negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

183. Postmeds also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

184. As a direct and proximate result of Postmeds' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

185. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

186. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

187. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Postmeds to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

188. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

189. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to Postmeds in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

190. Postmeds' Privacy Policy memorialized the rights and obligations of Postmeds and its patients. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

191. In the Privacy Policy, Postmeds commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

192. Plaintiffs and Class Members fully performed their obligations under their contracts with Postmeds.

193. However, Postmeds did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Postmeds breached its contracts with Plaintiffs and Class Members.

194. Postmeds allowed third parties to access, copy, and exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, Postmeds breached the Privacy Policy with Plaintiffs and Class Members.

195. Postmeds' failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Postmeds providing services to Plaintiffs and Class Members that were of a diminished value.

196. As a result, Plaintiffs and Class Members have been harmed, damaged, and injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

197. As a direct and proximate result of Postmeds' conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

198. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Postmeds to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

199. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

200. This Count is pleaded in the alternative to Count III above.

201. Postmeds provides digital pharmacy delivery services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the

provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

202. Through Defendant's sale of services to Plaintiffs and Class Members, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

203. As consideration, Plaintiffs and Class Members paid money to Postmeds and/or turned over valuable Private Information to Postmeds. Accordingly, Plaintiffs and Class Members bargained with Postmeds to securely maintain and store their Private Information.

204. Postmeds accepted payment and possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

205. In paying Defendant, either directly or indirectly, and providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiffs and Class Members intended and understood that Postmeds would adequately safeguard the Private Information as part of those services.

206. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

207. Plaintiffs and Class Members would not have entrusted their Private Information to Postmeds in the absence of such an implied contract.

208. Had Postmeds disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Postmeds.

209. As a provider of healthcare, Postmeds recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

210. Postmeds violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Postmeds further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

211. Additionally, Postmeds breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

212. Postmeds also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

213. Postmeds further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

214. Postmeds further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

215. Postmeds further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

216. Postmeds further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

217. Postmeds further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

218. Postmeds further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

219. Postmeds further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

220. Postmeds further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

221. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to Postmeds in exchange for Postmeds' agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

222. Plaintiffs and Class Members have been damaged by Postmeds' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

223. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

224. This Count is pleaded in the alternative to Counts II and III above.

225. Plaintiffs and Class Members conferred a benefit on Postmeds by turning over their Private Information to Defendant and by paying for medications and services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

226. Upon information and belief, Postmeds funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

227. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Postmeds.

228. Postmeds has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

229. Postmeds knew that Plaintiffs and Class Members conferred a benefit upon it, which Postmeds accepted. Postmeds profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

230. If Plaintiffs and Class Members had known that Postmeds had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

231. Due to Postmeds' conduct alleged herein, it would be unjust and inequitable under the circumstances for Postmeds to be permitted to retain the benefit of its wrongful conduct.

232. As a direct and proximate result of Postmeds' conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Postmeds' possession and is subject to further unauthorized disclosures so long as Postmeds fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

233. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Postmeds and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Postmeds from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

234. Plaintiffs and Class Members may not have an adequate remedy at law against Postmeds, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

235. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

236. In light of the special relationship between Postmeds and its patients, whereby Postmeds became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) Postmeds was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Postmeds' patients' Private Information was and is stored.

237. Postmeds had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its patients' relationship, in particular to keep the Private Information secure.

238. Postmeds breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

239. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Postmeds created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

240. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

241. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

242. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

243. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

244. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

245. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

246. Postmeds breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

247. As a direct and proximate result of Postmeds' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

248. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

249. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

250. Postmeds owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

251. Postmeds still possesses Private Information regarding Plaintiffs and Class Members.

252. Plaintiffs allege that Postmeds' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

253. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Postmeds owes a legal duty to secure its patients' Private Information and to timely notify customers of a data breach under the common law, HIPAA, and the FTCA;

b. Postmeds' existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' Private Information; and

c. Postmeds continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

254. This Court should also issue corresponding prospective injunctive relief requiring Postmeds to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order Postmeds to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Postmeds must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Postmeds' systems on a periodic basis, and ordering Postmeds to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Postmeds' systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

255. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Postmeds. The risk of another such breach is real, immediate, and substantial. If another breach at Postmeds occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

256. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Postmeds if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Postmeds' compliance with an injunction requiring reasonable prospective data security

measures is relatively minimal, and Postmeds has a pre-existing legal obligation to employ such measures.

257. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Postmeds, thus preventing future injury to Plaintiffs and other patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Postmeds to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Postmeds to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 7, 2023.

Respectfully submitted,

/s/ Kyle McLean

Kyle McLean (SBN #330580)
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739
E: kmclean@sirillp.com

Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com